A Survey Paper on Efficient Physical Intrusion Detection in Internet of Things

Surumi P.A
Department of computer science
St. Joseph's college (Autonomous)
Irinjalakuda, Thrissur, Kerala

Reesha P.U
Department of computer science
St. Joseph's college (autonomous)
Irinjalakuda, Trissur, Kerala

***Abstract*— The Internet of Things (IoT) is Associate in Nursing ever-growing network of sensible objects. It refers to the physical objects square measure capable of exchanging info with different physical objects. It introduces varied services and human's routine life depends on its out there and reliable activities. Therefore, the challenge of implementing secure communication within the IoT network should be addressed . The IoT network is secured with cryptography and authentication, however it can not be protected against cyber-attacks. Hence, the Intrusion Detection System (IDS) is required. during this paper, we have a tendency to discuss some security attacks and varied intrusion detection approaches to mitigate those attacks.**

Keyword- Internet of things ,intrusion detection system, Cyber attack

1 INTRODUCTION

Internet of Things (IoT) has attracted much research interest from the academia and industry for many critical military and civilian applications, including intrusion detection, surveillance, targeting systems, industrial process monitoring and traffic control. The main idea of IoT is that in the future most of the objects that surround us would be accessible, sensed, and interconnected inside the global, dynamic, living structure of the Internet . In a typical IoT network, the nodes are battery-powered microsystems that embed a variable number of transducers to monitor their surroundings. The nodes also embed a wireless radio and form a wireless network autonomously, through which they communicate their sensed data. Nodes also connect to the internet or to other external networks, and act as gateways to forward the sensed data to remote users.

An IoT network usually incorporates a large number of heterogeneous nodes, e.g., smart meters, cameras, vehicles, while providing untethered access to a variety of data generated

by such nodes to deliver new services to improve quality of daily lives. Depending on the particular application, in IoT networks, we can broadly classify data gathering pattern as time driven and event driven.

An IoT network for intrusion detection can be implemented for diverse security scenarios, ranging from search-and-capture missions (in military scenarios) within a region to a large battlefield . The performance of an Intrusion Detection System (IDS) is measured by how fast the intruder is detected by the nodes . An efficient security system is attained by deploying plenty of nodes. This results in efficient covering of the entire monitored region, making it possible for detection of any intruder once it invades any portion of the secured area.

I RELATED WORK

In the last decade, many intrusion detection (also, known as tracking or object/target detection) techniques were proposed to detect the intruder quickly and use energy efficiently in wireless resource constrained nodes. Most of the proposed intrusion detection techniques belong to WSN paradigm. Similar to WSN, nodes in IoT play an important role in collecting,sending, and receiving a signicant amount of data. Hence, in our work, most of the problems related to the intrusion detection techniques in WSNs paradigms are inherited in IoT as well. In this Section, we briey summarize the existing intrusion detection strategies most relevant in our context, particularly, the works aiming at effictively detecting the presence of an intruder and conserving network resources.

Researchers proposed several intrusion detection techniques in the literature under different metrics and assumptions. In one such work, Li et al. [1] analyzed the detection probability of crossing path across the barrier of nodes under probabilistic sensing model and random node deployment. Based on the analysis, they develop a scheduling algorithm to conserve the energy of nodes. Further, they extended the work by proposing a localization algorithm to provide the global barrier coverage energy-efficiently in [2]. However, the complexity of the algorithm depends on the node density along the barrier region. Diffeerent from [1,2],Zhao et al. [3] proposed an IDS for detecting the movement of intruders based on passive Radio Frequency Identiffication (RFID) tag. Basically, the proposed IDS measures the critical power variation sequences of passive tag in order to detect the real-time direction of moving intruders. Similarly, Han et al. [4] proposed a motion detection and tracking method for efficient intrusion detection using passive RFID tags. The work leverages the critical state phenomenon caused by interference of two adjacent tags to detect intruders. Unlike static network, the authors in [5] address the intrusion detection problem for mobile resource-constrained nodes

In our speciffic context of efficient intrusion detection technique for IoT, we have the following observations:

- Except [6], all of the above works consider intrusion

detection problem in a homogeneous network. Since IoT is typically heterogeneous in nature, investigation of intrusion detection problem in a homogeneous network is not adequate. Motivated by this fact, in this work, we examine intrusion detection problem in both homogeneous and heterogeneous network scenarios.

- Unlike existing works, we introduce a tailor-made Gaussian distribution which offers an improved sensing coverage without incurring additional communication, computation, and energy consumption overheads. Hence, our work is highly important for a network designer to design IoT for intrusion detection applications.
- To the best of our knowledge, we are the first to analyze the intrusion detection problem in both homogeneous and heterogeneous IoT, considering both single-sensing and multiple-sensing detection scenarios.
- We investigate the network coverage and connectivity issues in a heterogeneous IoT, which is the required condition to warrant the higher intrusion detection probability.
-

3 RELEVANT TERMS

This section introduces the central concepts of this paper: Intrusion Detection Systems and Internet of Things.

A. *Internet of Things*

The Internet of Things (IoT) may be a good network that connects all things to the net for the aim of exchanging info with united protocols . So, anyone will access something, at any time and from anyplace . In IoT network, things or objects are wirelessly connected with good small sensors. IoT devices will move with one another without human intervention . IoT uses distinctive addressing schemes to move with different objects/things and work with objects to form new applications or services. IoT introduces numerous applications like good homes, good cities,
health observance, good surroundings, and good water . With the event of IoT applications, there ar such a big amount of
issues raised. Among several different problems, security issue of IoT can't be unheeded. IoT devices are accessed from anyplace
via entrusted network just like the web therefore IoT networks are unprotected against a good vary of malicious attacks. If
security problems don't seem to be self-addressed then the guidance is also leaked at any time. Thus, the safety downside
must be self-addressed. the architecture of IoT is divided into three basic layers
1) application layer; 2) network layer; and 3)perception layer, which are further described below

- Perception layer: conjointly referred to as the detector layer, is carried out because the backside layer in IoT design. Its most important goals are to attach matters in to IoT network, and to live, collect, and method the country information associated to these items by deployed good devices, sending the processed data into greater layer by using layer interfaces.
- Network layer: It is additionally recognized as the transmission layer, is carried out as the center layer in IoT architecture . The community layer is used to receive the processed statistics supplied by perception layer and determine the routes to transmit the records and facts to the IoT hub, devices, and purposes through built-in networks. The network layer is the most necessary layer in IoT architecture, due to the fact more than a few units (hub switching, gateway, cloud computing perform etc.), and a number of conversation technologies (Bluetooth, Wi-Fi, long-term evolution, etc.) are integrated in this layer.

- Application layer: It is additionally known as the business layer, is applied as the pinnacle layer in IoT architecture . The application layer receives the data transmitted from community layer and makes use of the data to grant required services or operations. A number of purposes exist in this layer, each two having distinctive requirements.

[16] propose three useful topologies: point to point, star and mesh. The latter is decentralized, and preferable for IoT systems but the nodes have a higher consume of resources to maintain routing protocols to forward packets in addition to the main sensor tasks. The star topology doesn't need so much resources in the standard nodes but has a weakness in providing a single point of failure in IoT system due to the use of a unique gateway. Different alliances, consortiums, special interest groups, and standard development organizations have proposed a considerable amount of communication technologies for IoT,what may carry a big challenge for end-to-end security in IoT applications [17].Most popular technologies for IoT include infrastructureprotocols like IEEE 802.15.4, Bluetooth Low Energy (BLE),Wireless HART, Z-Wave, LoRaWAN, 6LoWPAN, DTLS andRPL, and application protocols like CoAP and MQTT (Message Queue Telemetry Transport).In cyber security, the Confidentiality – Integrity –Availability (CIA) triad is well known. Just a few of the surveyed papers however relate CIA back to IoT. BesidesCIA,[18] adds more features to be addressed like Identification and Authentication, Privacy and Trust. The Open Web Application Security Project (OWASP) also have a useful list of IoT Attack Surface Areas which they state should be understood by manufactures, developers, researchers and companies looking to deploy IoT in their organizations [19]. [18] and [20] outlinesome security challenges in each layer of IoT architecture presenting common vulnerabilities and attack

- **Perception layer**: As the main purpose of the perception layer in IoT it to collect data, the security challenges in this layer focus on forging collected data and destroying perception devices by the following attacks: node capture; malicious code injection;false data injection; replay or freshness; crypto analysis and side channel; eavesdropping and interference; and sleep deprivation.

- **Network layer**: As the main purpose of the network layer in IoT is to transmit collected data, the security challenges focus in the impact of the availability of network resources through the next attacks: denial of service (DoS); spoofing; sink hole;wormhole; man-in-the-middle (MITM); routing information ;sybil; and unauthorized access.

- **Application layer**: As the main purpose of application layer is to support services requested by users, challenges in this layer focus on software attacks like phishing attack and malicious virus/worm and malicious scripts.

.**B *Intrusion Detection System***

The concept of intrusion detection was first proposed by Anderson in the year of 1980 [21] and is introduced to network system by Heberlein in 1990 [22]. An IDS is a tool or mechanism used to prevent unauthorized access and to detect attacks against a system or a network by analyzing the activity I the network or in the system itself.

A typical IDS is composed of sensors, an analysis engine, and a reporting system. Sensors are positioned at different network places or hosts and their main task is to collect data. The data collected are sent to the analysis engine, which is responsible to examine the collected data and detect intrusions. If an intrusion is detected by analysis engine, the reporting system generates an alert to network administrator.

IDSs can be classified as Host-based IDS (HIDS) and Network-based IDS (NIDS). HIDS is attached to a device/host and monitors malicious activities occurring within the system. NIDS connects to one or more network segments and monitors network traffic for malicious activities. Unlike NIDS, the HIDS analyzes not only network traffic but also system calls, running processes, file-system changes, interprocess communication, and application logs.

IDS approaches may also be classified as signature-based, anomaly-based or specification based.

- **signature-based approaches**, IDSs discover assaults when system or community behavior fits an attack signature stored in the IDS internal databases. If any gadget or network activity matches with saved patterns/signatures, then an alert will be triggered. This strategy is correct and very superb at detecting regarded threats, and their mechanism is easy to understand. However, this method is ineffective to detect new attacks and variations of known attacks, due to the fact a matching signature for these assaults is still unknown [23][24].
- **Anomaly-based IDSs** compare the activities of a device at an immediately against a ordinary behavior profile and generates the alert on every occasion a deviation from regular behavior exceeds a threshold. This strategy is environment friendly to notice new attacks however, something that does not in shape to a ordinary behavior is considered an intrusion and getting to know the whole scope of the normal conduct is no longer a easy task. Thereby, this method However, there is one essential distinction between these methods

usually has excessive false effective rates [25][26]. To construct the normal conduct profile, researchers typically rent statistical techniques or laptop getting to know algorithms. Specification is a set of regulations and thresholds that outline the expected conduct for community factors such as nodes ,protocols, and routing tables. Specification-based approaches detect intrusions when network behavior deviates from specification definitions. Therefore, specification-based detection has the identical reason of anomaly-based detection: identifying deviations from normal behavior. However, there is one necessary difference between these methods: in specification-based approaches, a human expert should manually outline the guidelines of every specification [25][28][27].

Manually defined specs normally furnish lower false positive costs in contrast with the anomaly-based detection[25][28][27]. Besides, Specification-based detection structures do not need a education phase, for the reason that they can begin working immediately after specification setup [28]. However, manually

defined specs may also now not adapt to one of a kind environment sand ought to be time-consuming and error-prone [25][28][27]

4 INTRUSION DETECTION SYSTEM IN INTERNET OF THINGS

Over the recent years, several review articles have been published on IDSs for technologies related to IoT such as mobile ad hoc networks (MANETs) ([29]; [30]; [31]), wireless sensor networks (WSNs) ([33];[34];[27]), cloud computing ([32]) and cyber-physical systems (CPS) ([25]).

. Our literature review of IDS in IoT classify every work concerning the following features of IDS: detection method, placement strategy and security threat. To classify IDSs for IoT, we will use the taxonomy proposed by [35] with regard of the attributes: detection method, placement strategy and security threat. The select works are listed and classified in Table I. In our opinion, by performing this analysis, we would not only improve our knowledge on the referred topics, but also create more opportunities for future researches in development of IDS In IoT .

anomaly-based method and assume that botnets cause unexpected changes in the traffic of 6LoWAPN sensors. The proposed solution computes the average for three metrics to compose the normal behavior profile. When metrics from any node violate the computed averages, the system raises an alert.

TABLE 1

[1] SCIENTIFIC WORKS THAT STUDY IDS IN IOT

Work	***Placement strategy***	***Detection method***	***Security threat***
Cho et al. [36]	*Centralized*	*Anomaly-based*	Botnet
Le. et al. [37]	Hybrid	Specification based	Routing attack
Raza et al. [38]	Hybrid	Hybrid	Routing attack
Krimmling et al .[39]	-	Hybrid	Routing attack and Man-in the-middle
Cervants et al. [40]	Distributed	Hybrid	Routing attack
Le et al. [41]	Hybrid	Specification based	Routing attack
Shreenivas et al. [42]	Hybrid	Hybrid	Routing attack

In their 2011 work, Le et al. [37] followed the approach of organizing the network in regions. With this approach, they use
a hybrid placement strategy to build a backbone of monitor nodes, one per region. The function of monitor nodes is to sniff the communication from its neighbors and define whether a node is compromised. One of the advantages of this solution is that there is no communication overhead. The detection method used is specification-based focused on detecting RPL attack.

In 2013, Raza et al. [38] present an IDS for IoT named SVELTE whose objective is to detect sinkhole and selective forwarding attacks. This IDS had a hybrid placement strategy due to the participation of the border router and network nodes in the detection system. The border router runs IDS modules responsible to detect intrusions by analyzing RPL network data due to process intensive needs. On the other hand, network nodes are responsible for transmitting information to the border router, sending RPL network data and notifying about malicious traffic received. This work has also a hybrid approach on detection method, trying to balance the computing cost of the anomaly-based method and the storage cost of the signaturebased method.s

In 2014, Krimmling et al. [39] purpose a IDS for IoT. Although they did not indicate what placement strategy had been following, they tested a hybrid detection method combining signature-based and anomaly-based approach. The tests were done with their proposed evaluation framework and the results obtained show that each approach failed in detecting some attacks. For the authors, a combination of detection methodscould detect a higher number of attacks such as routing and Man in-the-Middle attacks.

In 2015, Cervantes et al. [40] proposed an IDS for IoT name INTI (Intrusion detection of Sinkhole attacks in 6LoWPAN for Internet of Things). The placement strategy followed was a distributed system since they used a hierarchical structure of nodes. Each node as a role in the system, and the main task is to monitor a superior node estimating its traffic patterns. The approach combines concepts of trust and reputation in a specification-based method with anomaly-based method to monitor the exchange of packets between nodes. When a node detects a sinkhole attack, it broadcasts a message to alert the other nodes.

In their 2016 work, Le et al. [41] design a lightweight IDS solution for IoT. Their hybrid placement strategy divides the network into small clusters. Each cluster has a cluster head that communicates with all other cluster members. The cluster head monitors the cluster members and had placed a IDS instance while the other cluster members only reports information to the cluster head. The border router had also placed an IDS instance and is responsible for tasks that need more computational resources. The authors use specification-based method extending their previous work [Le2011?????] on detection routing attacks. in 2017, Shreenivas et al. [42] propose a solution on IDS for IoT. Their work is an extension of SVELTE, the work presented by Raza et al. [Raza2013 ????]. With the objective of improving the security within 6LoWPAN networks, the authors extend SVELTE with an intrusion detection module that uses the ETX (Expected Transmissions) metric. In RPL, ETX is a link reliability metric and monitoring the ETX value can prevent an intruder from actively engaging 6LoWPAN nodes in malicious activities. They also propose geographic hints to identify malicious nodes that conduct attacks against ETX-based networks. Their experimental results show that compared with rank-only mechanisms the overall true positive rate increases when they combine the EXT and rank based detection mechanisms.

5 CONCLUSION

Internet of Things is an important part of the future due to its ability to connect physical objects to Internet in different application domains. Despite this, the security of IoT must be investigated and developed. However, as the resources of IoT devices are constrained, many security mechanisms are hard to be implemented to protect the security of IoT networks. As security mechanism, the IDS is one of the most important in traditional networks and should be used on IoT networks as well.
we presented a literature review about IDSresearch for IoT networks. In this review we analyze 20 worksthat were published between 2009 and 2017 that propose IDS solutions for IoT networks. We used a taxonomy based on characteristics like placement strategy, detection method and security threat. infancy and incipient. The works reviewed do not cover a lot of IoT technologies and cannot detect a large

variety of attacks. Considering that placement strategy and detection method are so important characteristics of IDSs, we can also conclude that the analyzed works do not reach a consensus on which are the more proper options for that characteristics in IDSs in IoT.

In terms of future work we, as a research team, believe that will be important that future research's should concentrate attention on reach a consensus on which are the proper placement strategy and detection method. Increase the attack detection variety and address more IoT technologies should be also important to achieve in future research's.

REFERENCES

[1] J. Li, J. Chen, T. H. Lai, Energy-e_cient intrusion detection with a barrier of probabilistic sensors, Proc. of 31st Annual IEEE International Conference on Computer Communications (INFOCOM) (2012) 118-126.

[2] J. Chen, J. Li, T. H. Lai, Energy-e_cient intrusion detection with a barrier of probabilistic sensors: global and local, IEEE Transactions on Wireless Communications 12(2013) 4742-4755.

[3] K. Zhao, C. Qian, W. Xi, J. Han, X. Liu, Z. Jiang, J. Zhao, EMoD: efficient motion detection of device-free objects using passive RFID tags, Proc. of IEEE 23rd International Conference Network Protocols (ICNP) (2015) 291- 301 .

[4] J. Han, C. Qian, X.Wang, D. Ma, J. Zhao, W. Xi, Z. Jiang, Z.Wang, Twins: device-free object tracking using passive tags, IEEE/ACM Transactions on Networking 24 (2016) 1605-1617.

[5] Y. Keung, B. Li, Q. Zhang, The intrusion detection in mobile sensor network, Proc. of 11th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc) (2010) 11-20.

[6] Y.Wang, X.Wang, B. Xie, D.Wang, D. P. Agrawal, Intrusion detection in homogeneous and heterogeneous wireless sensor networks, IEEE Transactions on Mobile Computing 7 (2008) 698-711.

[7] D. Zegzhda, T. Stepanova, "Achieving Internet of Things security via providing topological sustainability", 2015 Science and Information Conference (SAI), pp. 269-276, 2015.

[8] Meddeb, "Internet of Things standards: Who stands out from the crowd?", IEEE Communications Magazine, vol. 54, no. 7, pp. 40-47, Jul.2016.

[9] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol. 4, no.5, pp. 1125-1142, Oct. 2017.

[10] OWASPInternet of Things Project,https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf, accessed 19 December 2017

[11] F. A. Alaba, M. Othman, I. Hashem, and F. Alotaibi, "Internet of Things security: A survey", Journal of Network and Computer Applications,Volume 88, 2017, Pages 10-28.

[12] J. P. Anderson, "Computer security threat monitoring and surveillance",Technical report, James P. Anderson Company, Fort Washington,Pennsylvania, 1980.

[13] L. T. Heberlein, "A network security monitor," in Proceedings of theIEEE Computer Society Symposium, Research in Security and Privacy,pp. 296-303, Oakland, Calif, USA, 1990.

[14] J. Vacca, 2013. Computer and Information Security Handbook. MorganKaufmann, Amsterdam, 2013.

[15] H. Liao, C. Lin, Y. Lin, and K. Tung, "Intrusion detection system: acomprehensive review", Journal of Network and Computer Applications,36 (1), 16-24, 2013.

[16] R. Mitchell, and I. Chen, "A survey of intrusion detection techniques forcyber-physical systems", ACM Computing Surveys (CSUR), 46 (4), 55,2014.

[17] K. Scarfone, and P. Mell, "Guide to intrusion detection and preventionsystems (IDPS)", Technical report, National Institute of Standards andTechnology, special Publication 800-94, 2007.

[18] Butun, S. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks", Communications Surveys and Tutorials IEEE, 16 (1), 266-282, 2014

[19] J. Amaral, L. Oliveira, J. Rodrigues, G. Han, and L. Shu, "Policy andnetwork-based intrusion detection system for IPv6-enabled wirelesssensor networks," In: Communications (ICC), 2014 IEEE International Conference on, pp. 1796-1801, 2014.

[20] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks", IEEE Wireless Communications, 11 (1), 48-60, 2004.

[21] T. Anantvalee, and W. Jie, "A survey on intrusion detection systems in mobile ad hoc networks", Wireless Network Security, 2, 159-180, 2017.

[22] S. Kumar, and K. Dutta, "Intrusion detection in mobile ad hoc networks:techniques, systems, and future challenges", Security and Communication Networks, 9 (14), 2484-2556, 2016.

[23] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "Asurvey of intrusion detection techniques", in Journal of Network and Computer Applications, 36 (1), 42-57, 2013.

[23] A. Farooqi, and F. Khan, "Intrusion detection systems for wireless sensor networks: a survey", In Communication and Networking Communications in Computer and Information Science, 56, Springer,Berlin, Heidelberg, 234-241, 2009.

[24] A. Abduvaliyev, A. Pathan, Z. Jianying, R. Roman, and W. Wai-Choong2013, "On the vital areas of intrusion detection systems in wireless sensor networks", IEEE Communications Surveys & Tutorials,15 (3), 1223-1237, 2013.

[25] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga,"A survey of intrusion detection in internet of things," Journal of Networkand Computer Applications, vol. 84, pp. 25-37, 2017.

[26] E. Cho, J. Kim, and C. Hong, "Attack model and detection scheme forbotnet on 6LoWPAN," In Management Enabling the Future Internet for Changing Business and New Computing Services, Lecture Notes in Computer Science 5787. Springer, Berlin, Heidelberg, 515-518, 2009.

[27] A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based IDS for securing RPL from topology attacks," In: Wireless Days (WD), 2011 IFIP, pp. 1-3, 2011.

[28] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: real-time intrusion detection in the Internet of Things," Ad Hoc Network, 11 (8), 2661-2674,2013.

[29] J. Krimmling, and S. Peter, "Integration and evaluation of intrusiondetection for CoAP in smart city applications," In: Communications and Network Security (CNS), 2014 IEEE Conference on, pp. 73-78, 2014.

[30] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internetof Things," In: 2015 IFIP/IEEE International Symposium on IntegratedNetwork Management (IM), pp. 606-611, 2015.

[31] A. Le, J. Loo, K. Chai, and M. Aiash, "A specification-based IDS for detecting attacks on RPL-based network topology," Information, 7 (2),25, 2016.

[32] D. Shreenivas, S. Raza, and T. Voigt, "Intrusion Detection in the RPLconnected6LoWPAN Networks," Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, April 02-02,Abu Dhabi, United Arab Emirates, 2017.